



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/643,564	08/18/2003	Bruce McCorkendale	SYMC1032	4932

34350 7590 03/15/2007
GUNNISON, MCKAY & HODGSON, L.L.P.
1900 GARDEN ROAD, SUITE 220
MONTEREY, CA 93940

EXAMINER

KHOSHNOODI, NADIA

ART UNIT	PAPER NUMBER
----------	--------------

2137

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/15/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/643,564

Applicant(s)

MCCORKENDALE ET AL.

Examiner

Nadia Khoshnoodi

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) ____ is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 18 August 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. ____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|--|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date <u>1/9-26-2003</u> | 6) <input type="checkbox"/> Other: ____ |

DETAILED ACTION

Claim Objections

Claim 6 is objected to because of the following informalities: it recites “an destination port” where it should be “a destination port”. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1 and 3-6 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter, as the result of these claims is not in a tangible form. Rather, the claimed limitations merely contain steps for comparing and determining if the code is malicious without carrying out any steps/operations based on those results which is necessary to yield a tangible result. In order to meet the “useful” requirement, there must be some application implemented based on the results. For example, claim 2 is not rejected under 35 U.S.C 101 since the tangible/useful result is the step of “providing a notification of the malicious code detection” once the malicious code is detected.

Claims 12-14 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter, since the result of these claims is not useful as claimed. Rather, the claimed limitations merely contain system components associated with one another without carrying out any steps/operations which yield a malicious code detection device (since nowhere in the claim is there any reference to detecting malicious code from the comparator’s results). More specifically, Applicants have merely claimed an interception function, two memories, each

of which is in communication with a comparator, without specifying how these components interact with one another to form a malicious code detection device as set forth in the preamble of the claim.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 12-14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, claim 12 states that a "malicious code detection device" comprising various limitations is being claimed. However, there are no limitations in the body of the claim which specify how the malicious code is detected.

Claim Rejections - 35 USC § 102

I. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

II. Claims 1-7 and 12-14 are rejected under 35 U.S.C. 102(b) as being fully anticipated by Hockey, WO 02/19069 A2.

As per claim 1:

Hockey teaches a method comprising: comparing outbound traffic on a host computer system to inbound traffic on the host computer system (pg. 19, line 10 – pg. 20, line 3); and determining if malicious code is detected on the host computer system based on the comparing (pg. 20, line 26 – pg. 21 line 30)

As per claim 2:

Hockey teaches the method of claim 1. Furthermore, Hockey teaches the method further comprising: if malicious code is detected, providing a notification of the malicious code detection (pg. 21, lines 22-30).

As per claim 3:

Hockey teaches the method of claim 1. Furthermore, Hockey teaches the method wherein the comparing is performed using a similarity comparison technique (pg.21, lines 4-14).

As per claim 4:

Hockey teaches the method of claim 1. Furthermore, Hockey teaches the method wherein at least a portion of the outbound traffic is compared to at least a recently received portion of the inbound traffic, the at least a portion of the outbound traffic being subsequent in time to the at least a recently received portion of the inbound traffic (pg. 19, line 10 – pg. 20, line 3).

As per claim 5:

Hockey teaches the method of claim 1. Furthermore, Hockey teaches the method wherein the inbound traffic is received at the host computer system from a source port, and wherein the outbound traffic is for sending to a destination port, and further wherein the source port and the destination port are the same port (pg. 21, lines 4-14).

As per claim 6:

Hockey teaches the method of claim 1. Furthermore, Hockey teaches the method wherein the inbound traffic is received on the host computer system from a source port, and wherein the outbound traffic is for sending to a destination port, and further wherein the source port and the destination port are different ports (pg. 22, lines 1-16).

As per claim 7:

Hockey teaches the method of claim 2. Furthermore, Hockey teaches the method further comprising: implementing protective actions (pg. 21, lines 22-35).

As per claim 12:

Hockey teaches a malicious code detection device comprising: an interception function (pg. 17, lines 1-5); at least one inbound traffic memory area coupled to the interception function (pg. 19, lines 22-25); at least one outbound traffic memory area coupled to the interception function (pg. 17, lines 5-10); and a comparator coupled to the at least one inbound traffic memory area and the at least one outbound traffic memory area (pg. 19, line 10 – pg. 20, line 3).

As per claim 13:

Hockey teaches the malicious code detection device of claim 12. Furthermore, Hockey teaches the method further comprising: a prior name resolution correlation function (pg. 20, line 25 – pg. 21, line 2).

As per claim 14:

Hockey teaches the malicious code detection device of claim 13. Furthermore, Hockey teaches the method wherein the prior name resolution correlation function is included in the interception function (pg. 20, line 26 – pg. 21, line 2).

Art Unit: 2137

III. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

IV. Claims 15-24 are rejected under 35 U.S.C. 102(e) as being fully anticipated by Chesla et al., US Pub. No. 2004/0250124.

As per claim 15:

Chesla et al. teach a method comprising: intercepting inbound traffic on a host computer system (par. 121); copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic (par. 365-370); releasing the inbound traffic (par. 353-355); intercepting outbound traffic on the host computer (par. 149); copying the outbound traffic to an outbound traffic memory area, the copying the outbound traffic generating copied outbound traffic (par. 300); releasing the outbound traffic (par. 353-355); comparing at least a portion of the copied inbound traffic with at least a portion of the copied outbound traffic (par. 137); determining if malicious code is detected on the host computer system based on the comparing (par. 137); and if malicious code is detected, providing a notification of the malicious code detection (par. 435).

As per claim 16:

Chesla et al. teach the method of Claim 15. Furthermore, Chesla et al. teach wherein the comparing is performed using a similarity comparison technique (par. 159).

As per claim 17:

Chesla et al. teach the method of claim 15. Furthermore, Chesla et al. teach wherein the at least a portion of the copied outbound traffic is subsequent in time to the at least a portion of the copied inbound traffic (par. 159).

As per claim 18:

Chesla et al. teach the method of claim 15. Furthermore, Chesla et al. teach the method further comprising: prior to the copying the outbound traffic, if the outbound traffic correlates to a prior name resolution lookup performed on the host computer system, releasing the outbound traffic (par. 134 and 289).

As per claim 19:

Chesla et al. teach the method of claim 15. Furthermore, Chesla et al. teach wherein the inbound traffic is copied to the inbound traffic memory area on a per port basis (par. 189), and wherein the outbound traffic is copied to the outbound traffic memory area on a per destination port basis (par. 295).

As per claim 20:

Chesla et al. teach a method comprising: intercepting inbound traffic on a host computer system (par. 121); copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic (par. 264); releasing the inbound traffic (par. 353-355); intercepting outbound traffic on the host computer (par. 149); buffering the outbound traffic in an outbound traffic memory area, the buffering the outbound traffic generating buffered outbound traffic (par. 149); comparing at least a portion of the copied inbound traffic with at least a portion of the buffered outbound traffic (par. 137 and 159); determining if malicious code is detected on the host computer system based on the comparing

(par. 137); if malicious code is detected, providing a notification of the malicious code detection (par. 354); and if malicious code is not detected, releasing the at least a portion of the buffered outbound traffic (par. 160).

As per claim 21:

Chesla et al. teach the method of claim 20. Furthermore, Chesla et al. teach wherein the comparing is performed using a similarity comparison technique (par. 159).

As per claim 22:

Chesla et al. teach the method of Claim 20. Furthermore, Chesla et al. teach wherein the at least a portion of the buffered outbound traffic is subsequent in time to the at least a portion of the copied inbound traffic (par. 159).

As per claim 23:

Chesla et al. teach the method of claim 20. Furthermore, Chesla et al. teach the method further comprising: prior to buffering the outbound traffic, if the outbound traffic correlates to a prior name resolution lookup performed on the host computer system, releasing the outbound traffic (par. 134 and 289).

As per claim 24:

Chesla et al. teach the method of claim 20. Furthermore, Chesla et al. teach wherein the inbound traffic is copied to the inbound traffic memory area on a per port basis (par. 189), and wherein the outbound traffic is buffered in the outbound traffic memory area on a per destination port basis (par. 295).

V. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

VI. Claims 8-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hockey, WO 02/19069 A2 as applied to claim 2 above, and further in view of Chesla et al., US Pub. No. 2004/0250124.

As per claim 8:

Hockey substantially teaches the method of claim 2. Hockey further teaches that a message digest may be stored when the traffic is intercepted (pg. 17, line 33 – pg. 18, line 17). Not explicitly disclosed is the method further comprising: intercepting the inbound traffic; copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic; releasing the inbound traffic; intercepting the outbound traffic; copying the outbound traffic to an outbound traffic memory area, the copying the outbound traffic generating copied outbound traffic; and releasing the outbound traffic. However, Chesla et al. teach that copies of values of the incoming traffic/outgoing traffic may be stored in both inbound and outbound directions in order to allow for detecting possible attacks. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hockey to store a copy of the inbound and outbound traffic in different memory areas in order to determine if a possible flooding attack (as one example) is underway. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Chesla et al. suggest

Art Unit: 2137

that using a list of incoming/outgoing signatures and monitoring that list closely (while still releasing the traffic) provides a great technique for various attack detections on a network in par. 353-355.

As per claim 9:

Hockey and Chesla et al. substantially teach the method of claim 8. Furthermore, Chesla et al. teach wherein the comparing comprises: comparing at least a portion of the copied inbound traffic with at least a portion of the copied outbound traffic.

As per claim 10:

Hockey substantially teaches the method of claim 2. Not explicitly disclosed is the method further comprising: intercepting the inbound traffic; copying the inbound traffic to an inbound traffic memory area, the copying the inbound traffic generating copied inbound traffic; releasing the inbound traffic; intercepting the outbound traffic; buffering the outbound traffic in an outbound traffic memory area, the buffering the outbound traffic generating buffered outbound traffic; and if malicious code is not detected releasing the buffered outbound traffic. However, Chesla et al. teach that copies of values of the incoming traffic/outgoing traffic may be stored in both inbound and outbound directions in order to allow for detecting possible attacks. Furthermore, Chesla et al. teach wherein buffering techniques may be used on outgoing traffic to lower the rate at which the traffic can continue on to its final destination. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Hockey to store a copy of the inbound and outbound traffic in different memory areas in order to determine if a possible flooding attack (as one example) is underway, as well as to buffer the outgoing traffic. This modification would have been obvious because a person

Art Unit: 2137

having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Chesla et al. suggest that using a list of incoming/outgoing signatures and monitoring that list closely (while still releasing the traffic) provides a great technique for various attack detections on a network in par. 353-355. Furthermore, Chesla et al. suggest that buffering the traffic can lessen the impact of an attack, since by buffering the outgoing traffic the system allows for lowering the rate at which the traffic can proceed in par. 149.

As per claim 11:

Hockey and Chesla et al. substantially teach the method of claim 10. Furthermore, Chesla et al. teach wherein the comparing comprises: comparing at least a portion of the copied inbound traffic with at least a portion of the buffered outbound traffic (par. 149).

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. **US Pub. No. 2003/0154255** has been cited because it is relevant due to the manner in which the invention has been claimed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

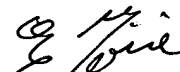
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Nadia Khoshnoodi
Examiner
Art Unit 2137
3/10/2007

NK



EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER